

REMARKS

Claims 1-5 were examined. All claims were rejected. In response to the above-identified Office Action, Applicants amend claims 1 and 3-5, but do not cancel any claims or add any new claims. Reconsideration of the rejected claims in light of the aforementioned amendments and the following remarks is requested.

I. Regarding The Specification

The Examiner again reminded Applicants of the proper format for the Abstract of the disclosure. In the Response to Office Action mailed September 24, 2004, Applicants supplied a replacement Abstract that was believed to be in the proper form. Perhaps that paper was inadvertently lost or misplaced. Applicants submit herewith a copy of the previously-presented replacement Abstract. The Examiner's approval is respectfully requested.

II. Claims Rejected Under 35 U.S.C. § 112, Second Paragraph

The Examiner rejected claims 1 and 2 under 35 U.S.C. § 112, second paragraph, as incomplete for omitting essential steps. Specifically, the Examiner indicates a failure to describe what is done with the random number selected by the client in step (b) of claim 1. Applicants have amended claim 1 to remove references to that random number, and to clearly identify other random numbers mentioned. It is believed that these amendments correct the incompleteness noted by the Examiner, so withdrawal of these rejections is requested.

The Examiner also rejected claim 3 under 35 U.S.C. § 112, second paragraph, as indefinite for failing to particularly point out and distinctly claim material which applicants regard as their invention. Specifically, the Examiner indicates that the term r_b in the equation $x = (g^b)^{A+r_b}$ was not defined. Applicants' amendments to claim 3 make clear that r_b is a random number sent to the client, while r_A is a random number selected by the client. These amendments are believed to address the Examiner's concerns, and withdrawal of the rejection of claim 3 is requested.

III. Comments on § 102(b) and § 103(a) Rejections

The Examiner rejects claim 1 under 35 U.S.C. § 102(b) as anticipated by U.S. Patent No. 5,748,740 issued to Curry *et al.* ("*Curry*"), rejects claim 4 under 35 U.S.C. § 102(b) as anticipated by Applied Cryptography, Second Edition (1996) by Bruce Schneier ("*Schneier*"), and claims 2, 3 and 5 under U.S.C. § 103(a) as unpatentable over U.S. Patent No. 5,910,989 issued to Naccache ("*Naccache*") in view of Curry. However, the present invention is entirely distinguishable from the cited reference for the following reasons.

In the present invention, the client encrypts a random number r_B received from the server based on the server's public key in order to check whether the client generates a ciphertext under an appropriate protocol. In other words, for defeating denial-of-service attacks on authentication protocols, the client is verified by generating and sending the ciphertext based on the random number r_B and the server's public key.

On the contrary, Curry teaches the service provider (*i.e.* not the client as disclosed in the present invention) encrypts a random number r_B received from the portable module (not the server as disclosed in the present invention) in order to check whether the service provider is secure.

However, Curry and Naccache fail to teach encrypting the random number r_B received from the server and returning the encrypted data to the server. In other words, Curry does not disclose a system for defeating denial of service attacks on authentication protocols.

IV. Claims Rejected Under 35 U.S.C. § 102(b)

The Examiner rejected claim 1 under 35 U.S.C. § 102(b) as anticipated by Curry, *supra*.

Claim 1 recites a method comprising several steps in an interaction between a client and a server. The final claimed step is comparing a recovered random number r_B' to a random number r_B sent to the client, and providing a service to the client if the numbers are equal. The comparison is to happen at the server. In the Examiner's analysis, however, the final step is said to be taught by the service provider (which had been aligned with the claimed client) providing service to the module (which had been aligned with the claimed server). In other words, the two entities that allegedly perform the claimed method suddenly switch roles at the last step. This switch defeats

the Examiner's *prima facie* case of anticipation, because a § 102(b) reference must disclose each and every element of the rejected claim, arranged as stated in the claim. Since *Curry*'s module and service provider are arranged differently, Applicants respectfully submit that the reference fails to anticipate the claim, and request that the Examiner withdraw the rejection.

Claim 4 is also mentioned in the discussion of *Curry* and claim 1, but the rejection of claim 4 appears to be made solely over the *Schneier* reference. However, Applicants observe that *Curry* fails to anticipate claim 4 for at least the same reason that it fails to anticipate claim 1: *Curry*'s module and service provider cannot be consistently aligned with the claimed server and client, because the entity that provides service does not also perform the other steps claimed to be done at the server.

The Examiner rejected claim 4 under 35 U.S.C. § 102(b) as anticipated by *Schneier*, *supra*.

Claim 4 recites a computer-readable medium for recording a program implementing a number of functions, including (b) at the server, receiving a ciphertext which is produced by the client based on the random number r_B' sent to the client, enciphered with the public key of the server. The portion of *Schneier* cited teaches only "mak[ing] *some computation* based on the random numbers" (emphasis added), and omits that "some computation" is (or should be) the claimed enciphering with the public key of the server. Since there are an infinite number of computations that could be made on a random number, and since *Schneier* explicitly teaches away from the claimed computation of the client encrypting a random number from a server (*see, e.g., Schneier* p. 54, third paragraph: "[i]t is foolish to encrypt arbitrary strings – not only those sent by untrusted third parties, but under any circumstances at all."), Applicants respectfully submit that the protocol described in *Schneier* at p. 54, ¶ 4, fails to anticipate the claimed program's functions. For at least these reasons, the Examiner is requested to withdraw the rejection of claim 4.

V. Claims Rejected Under 35 U.S.C. § 103(a)

The Examiner rejected claims 2, 3 and 5 under 35 U.S.C. § 103(a) as unpatentable over U.S. Patent No. 5,910,989 issued to Naccache ("*Naccache*") in view of *Curry*, *supra*.

Claim 2 depends upon claim 1, discussed above. *Naccache* is relied upon in this rejection solely for the element of hashing a secret master key and an index parameter

for a random number, and Applicants' review of *Naccache* fails to reveal any teaching or suggestion of the elements of claim 1 already noted to be missing from *Curry*. Thus, claim 2 is believed to be patentable for at least the reasons discussed in relation to claim 1. Applicants respectfully request that the Examiner withdraw the rejection of claim 2.

Claim 3 recites a method for defeating a denial-of-service attack comprising a number of steps to be performed by a server, culminating in the possible provision of service by the server to the client. Claim 5 recites a server authentication system comprising a computer-readable medium to contain a program to implement various functions, including at the server, receiving values computed by the client according to a specified formula, and possibly providing service from the server to the client. The Examiner's analysis in connection with the rejections of claims 3 and 5 is brief, but appears to rely upon the alleged teaching in *Curry* of the same steps performed by *Curry*'s module and service provider. However, as already noted, *Curry*'s entities cannot consistently be likened to the claimed server and client, because the claimed server provides a service to the client, and the claimed client computes a value by enciphering a random number with the server's public key. In *Curry*, the entity that provides the service (the service provider) *also* computes the value. *Naccache* also fails to resolve the differences between the claimed methods and *Curry*'s teachings. For at least these reasons, Applicants respectfully request that the rejections of claims 3 and 5 be withdrawn.

The Examiner rejected claims 3 and 5 under 35 U.S.C. § 103(a) as unpatentable over *Naccache, supra*, in view of *Schneier, supra*. However, as discussed above, *Schneier* teaches a different protocol than that described by the rejected claims, and explicitly discourages the claimed methods. *Naccache*, too, is unavailing on those points. Consequently, Applicants request that these rejections of claims 3 and 5 be withdrawn.

The Examiner reiterated the rejection of claims 1-5 under 35 U.S.C. § 103(a) as unpatentable over "Client Puzzles: A Cryptographic Countermeasure Against Connection Depletion Attacks" by Juels *et al.* ("*Juels*"). Applicants respectfully traverse this rejection based upon the previously-presented argument, namely, that *Juels* merely describes the general contours of the problem and possible solutions, but does not teach or suggest the specific methods and functions claimed.

CONCLUSION

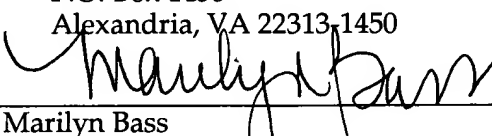
In view of the foregoing, it is believed that all claims now pending, namely claims 1-5, patentably define the subject invention over the prior art of record, and are in condition for allowance and such action is earnestly solicited at the earliest possible date. If the Examiner believes that a telephone conference would be useful in moving the application forward to allowance, or in correcting any remaining non-conformities in the proposed amended Abstract, the Examiner is encouraged to contact the undersigned at (310) 207-3800.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAPMAN, LLP

Dated: July 13, 2005


Eric S. Hyman, Reg. No. 30,139

<p>12400 Wilshire Boulevard Seventh Floor Los Angeles, California 90025 (310) 207-3800</p>	<p style="text-align: center;"><u>CERTIFICATE OF MAILING</u></p> <p>I hereby certify that the correspondence is being deposited with the United States Postal Service, with sufficient postage, as first class mail in an envelope addressed to:</p> <p style="text-align: center;">Mail Stop RCE Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450</p> <p> Marilyn Bass</p> <p style="text-align: right;">July 13, 2005</p>
---	---